

DMDC Computing Environments

The major components of DMDC's IT environment are described in the following sections. The technology stack is continuously upgraded once new versions of hardware/software are deemed by DMDC to be stable. The version levels outlined below represent the current and immediate version levels. Over the course of the contract, the contractor shall ensure that software applications are upgraded to ensure that they run on supported versions of the infrastructure.

DMDC Desktop Environment

DMDC infrastructure includes approximately 950 desktop PCs. The DMDC standard desktop environment is primarily PC class machines with Intel chip-based processing. The typical desktop configuration includes Compact Disc (CD) and Digital Video Disc (DVD). DMDC uses smart card reading devices at each desktop PC to support Public Key Infrastructure (PKI) login with the Common Access Card (CAC). Desktops run commercial off-the-shelf (COTS) software (operating systems, data base management systems, and office automation software, and DMDC-developed applications.

DMDC Networks

DMDC operates/supports several Ethernet local area networks (LANs) on both the West Coast and the East Coast. Over 500 personal computers (PCs) are located at DMDC-West (including a Classified Lab) and over 450 PCs at five different sites in Northern Virginia and one site in Auburn Hills, MI. The LANs are connected to each other (the Pentagon, the Auburn Hills System Management Center (AHSMC), the Naval Postgraduate School (NPS), and the Non-classified (but sensitive) Internet Protocol Routing Network (NIPRNET)) via T-1 lines and routers which define the DHRA/DMDC Wide Area Network (WAN). A separate LAN operates within the classified laboratory and is connected to the Secret Internet Protocol Router Network (SIPRNET). Network security is provided by router access lists and firewalls. DMDC also maintains data on IBM mainframe processors at NPS.

DMDC Data Center

DMDC's Data Center is a combination of government and government-owned contractor operated (GOCO) facilities.

DMDC Computing Environments

SUN Solaris Environment.

SUN systems perform as database servers and application servers. Most DMDC enterprise databases operate on Sun Enterprise 15k's, 6900's, or M9000 platforms. DMDC-West and Auburn Hills each maintain components of the DMDC Unix-platform production infrastructure, which are configured with the Sun Microsystems Operating System (Solaris 9, and 10) or Redhat Linux. DMDC also operates more than 300 additional SUN servers for various infrastructure and administrative purposes.

Web Servers and Application Servers

DMDC utilizes Sun and Oracle web servers in a web farm. In front of the web servers, DMDC utilizes F5 load balancers. DMDC utilizes a number of application servers including Oracle 10g/Oracle 11g, Sun, and Tomcat. Apache is utilized for some third party software but is not considered a DMDC accepted development platform.

Oracle Databases

The Oracle Relational Database Management System is DMDC's enterprise solution for data storage, manipulation and retrieval. DMDC currently maintains several Oracle databases, all of which reside and operate from Unix platforms. Mission critical databases are maintained at two separate geographic locations (Auburn Hills, MI and Seaside, CA). DEERS is recognized as the "definitive data source of identity and the verification of affiliation with the Department of Defense" (DoD Directive 1000.25, July 19, 2004). DEERS is a person centric Oracle 10g/11g database with satellites. The database exceeds 1.5 tera plus, houses 39+ million people. Current application service level agreements require sub second response times, 24/7/365 operations with 6 hours of scheduled downtime per month and high volumes (2.7+ transactions per day). DEERS generally has 2 major database releases per year for new model changes. The Authentication Data Repository (ADR) contains a subset of current data that is replicated on a real-time basis from the Defense Enrollment Eligibility Reporting System (DEERS) Person Data Repository (PDR) and the DEERS Medical Satellite Database (formerly the National Enrollment Database). ADR has approximately 100 person attributes

DMDC Computing Environments

(i.e., name, SSN, DOB, address) and personnel attributes (i.e., rank, service, assigned unit, benefits).

APPLICATION ENVIRONMENTS

All application development must comply with DMDC approved reference architectures. Some of the relevant approved reference architectures are summarized below.

DMDC Web Development

Java Web

Java based web sites utilize industry standard J2EE technologies in conjunction with DMDC approved third party components, including commercial off the shelf (COTS) and open source. Software used in the development of the DMDC Portals includes portlets written in JAVA. Oracle WebCenter (10g/11g) software is being used to integrate the various portlets displayed within the Portal. Authentication to the DMDC portals includes the use of the CAC, DFAS PIN, and DMDC's DSLogon credential. Portlets must be JSR 168/286 and WSRP 1.0/2.0 compliant. Portlets are currently being consumed by DMDC portals and external portals (e.g. e-Benefits). The following technologies are currently supported within the DMDC Java web GUI environment:

- Struts Framework
- Sun Java Server Faces
- Oracle ADF Faces
- MyFaces JSF Framework
- Trinidad JSF Framework
- Facelets JSF Framework
- Spring Web Flow Framework
- Portlet - Producer Framework
- Portlet - Consumer Framework

DMDC Computing Environments

Development Environment

Java web development is currently supported within DMDC on the Microsoft Windows XP platform. Supported Java Developer Kits (JDKs) range from 1.4.x to 1.5.x versions. Oracle's JDeveloper Integrated Development Environment (IDE) is used to develop Java web applications. Concurrent Versioning System (CVS) is used as the source code repository. Development testing is performed using the integrated Oracle application server included in JDeveloper.

Deployment of Java web applications is currently supported within DMDC on the following platforms:

- Oracle 11G Application Server (Linux OS)
- Oracle 13G Application Server (Linux OS)

Oracle PL/SQL Web

Oracle PL/SQL web applications are typically developed as stored procedures called via web browser over the http protocol. The following characteristics are quoted from the Oracle developer guide:

Visiting a web page, following a hypertext link, or pressing a Submit button on an HTML form causes the database server to run a stored procedure.

Any choices that a user makes on an HTML form are passed as parameters to the stored procedure. Parameters can also be hardcoded in the URL used to invoke the stored procedure. The results of the stored procedure are printed as tagged HTML text and are displayed in the browser as a web page. Web pages generated this way are dynamic: code runs inside the database server, producing HTML that varies depending on the database contents and the input parameters.

Development Environment

Oracle PL/SQL web development is currently supported within DMDC on the Microsoft Windows XP platform.

Deployment Environment

Deployment of PL/SQL web applications is currently supported within DMDC on the Oracle HTTP Server (to serve up the HTML pages to the Browser) and Oracle

DMDC Computing Environments

Database (where the Web pages are generated dynamically by the Oracle PL/SQL packages) running on a UNIX Operating system.

DMDC Data Access Services

Aion Data Server

Aion Knowledge Bases (KBs) are Aion®-written programs translating textual data to Interface Objects exchanged with the C cores (DMDC developed Pro*C component that accesses the Oracle database PL/SQL stored procedures to retrieve and update data). This layer of the architecture houses the business rules. Most of their behavior is common, and is often implemented as reusable modules. The specific behavior to each KB mainly resides in the specificity of the data's format and business rules. Aion is being phased out. Development Environment Aion data server development is currently supported within DMDC on the Microsoft Windows XP platform.

Deployment Environment

Deployment of Aion KBs is currently supported within DMDC on the UNIKIX MTP (Mainframe Transaction Processing) platform running on a UNIX Operating System.

J2EE Web Services

DMDC hosts and administers a number of web services. Some are for internal DMDC use while others are hosted for other agencies. Users are inside, as well as outside the DMDC LAN/WAN boundary. The browser based applications allow access to DMDC through securely architected channels using an Internet browser (e.g., Netscape or Internet Explorer) on the users' PCs. System to system interfaces are supported for some services. The following technologies are currently supported within the DMDC Java web services environment:

- Oracle10g R2 JAX-RPC Web Service (Sun Implementation JWSDP1.3, WSDL-Based)
- Oracle10gR3 JAX-RPC Web Service (Oracle Implementation J2EE1.4, WSDL-Based)

DMDC Computing Environments

- Oracle 11g JAX-RPC Web Service (Oracle Implementation J2EE1.4, WSDL-Based)

Development Environment

J2EE web services development is currently supported within DMDC on the Microsoft Windows XP platform. JDeveloper Integrated Development Environment (IDE) is used to develop Java web services. Concurrent Versioning System (CVS) is used as the source code repository. Supported Java Developer Kits (JDKs) range from 1.4.x to 1.5.x versions. Development testing is performed using the integrated Oracle application server included in JDeveloper.

Deployment Environment

Deployment of J2EE Web Services is currently supported within DMDC on the following platforms:

- Oracle 10G R2 Application Server (Unix OS)
- Oracle 10G R3 Application Server (Linux OS)
- Oracle 11G Application Server (Linux OS)

Reporting Applications

Cognos Web Reporting Applications

DMDC uses the industry leader reporting tool COGNOS to develop web-based reporting applications.

Development Environment

Cognos reporting development is currently supported within DMDC on the Microsoft Windows XP platform for data modeling (COGNOS Framework Manager modeling tool). Report Authoring is performed using the web-based Report Studio running on the Oracle 10G R3 (Linux OS).

DMDC Computing Environments

Deployment Environment

Report Applications are deployed via the Cognos Administration Web Interface. The COGNOS Server running on the Oracle 10G R3 (Linux OS) presents web-based report applications.

Jaspersoft Web Reporting Applications

JasperDecisions provides tools for report developers with different levels of expertise, experience, and authorization. It also provides a Web-based tool for end users to easily develop their own ad hoc reports. Jaspersoft is being phased out.

Development Environment

Jaspersoft reporting applications development is currently supported within DMDC on the Microsoft Windows XP platform. JDeveloper Integrated Development Environment (IDE) is used to develop Java web reporting applications by integration with the Jaspersoft COTS product (using the jaspersoft API). Reports are developed to produce a Scopeserver process Report Definition Language (RDL) files that run against data stored in the reporting database. Concurrent Versioning System (CVS) is used as the source code repository.

Deployment Environment

Report Definition Language (RDL) files are deployed into Jaspersoft's Scopeserver running in the Tomcat web container environment (UNIX OS).

Mainframe Environment

Current DMDC Mainframe OS System: z/OS 1.9

The DMDC mainframe computer is capable of single task computational speed (usually defined as MIPS — Millions of Instructions Per Second) and is also known for its redundant internal engineering and resulting high reliability and security, extensive input-output facilities, strict backward compatibility with older software, and high utilization rates to support massive throughput. Other typical aspects of the mainframe environment consist of:

DMDC Computing Environments

- Parallel Processing: Software upgrades are only non-disruptive when using z/OS and Parallel Sysplex, with workload sharing so one system can take over another's application while it is being refreshed.
- That mainframe is defined by high availability: The term Reliability, Availability and Serviceability (RAS) is a defining characteristic of mainframe computers.
- The mainframe has the ability to run (or host) multiple operating systems, and thereby operate not as a single computer but as a number of virtual machines.
- The mainframe can add or hot swap system capacity non disruptively and granularly. Modern mainframes, notably the IBM zSeries, System z9 and System z10 servers, offer two levels of virtualization: logical partitions (LPARs, via the PR/SM facility) and virtual machines (via the z/VM operating system).
- Batch Processing: The mainframe was designed to handle very high volume input and output (I/O) and emphasize throughput computing. High-throughput computing (HTC) is a computer science term to describe the use of many computing resources over long periods of time to accomplish a computational task. Compared to a typical PC, mainframes commonly have hundreds to thousands of times as much data storage, and can access it much faster.
- The mainframe also has execution integrity characteristics for fault tolerant computing. For example, z900, z990, System z9, and System z10 servers effectively execute result-oriented instructions twice, compare results, arbitrate between any differences (through instruction retry and failure isolation), then shift workloads "in flight" to functioning processors, including spares, without any impact to operating systems, applications, or users.

DMDC Computing Environments

- The mainframe tends to have numerous ancillary service processors assisting its main central processors (for cryptographic support, I/O handling, monitoring, memory handling, etc.) so that the actual "processor count" is much higher than would otherwise be obvious.

Security Specifications: Mainframe System design intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security--that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized.

z/OS V1.9 has enhanced PKI Services and RACF to help improve the creation, authentication, renewal, and management of digital certificates for user and device authentication. In addition, the z/OS Integrated Cryptographic Service Facility (ICSF) is planned to be enhanced to include the PKCS#11 standard. ICSF is part of the base of z/OS mainframe encryption, which enables you to encrypt and decrypt data, generate and manage cryptographic keys, and perform other cryptographic functions dealing with data integrity and digital signatures. By adopting the PKCS#11 standard the strength of mainframe encryption and secure centralized key management can be brought to and used by Web-based application and networking environments more easily.

z/OS V1.9 adds additional security enhancements, such as: additional exploiters for Application Transparent-TLS (AT-TLS), enhancements to PKI Services and RACF digital certificates, Network Authentication Support for AES, and enhanced System SSL support.

DMDC Computing Environments

The z/OS Communications Server uses a Policy Agent to centrally collect and distribute network settings you define in a simplified, centralized, manageable, and auditable manner.

Defense Biometric Identification System (DBIDS)

The Defense Biometric Identification System (DBIDS) is a DoD system developed by DMDC as a force protection and identity management program to manage personnel, property and installation access. It is a networked client server database system designed to easily verify the access authorization of personnel entering military installations by the use of machine-based authentication technologies and biometric identification. The program supports the adding, retrieving, updating and displaying of information on individuals who require military installation access. It produces installation passes (DBIDS cards) for personnel who are entitled to recurring and unescorted access to military installations and who do not possess a DoD ID Card. Registration functionality includes the registration of DoD and non-DoD ID cardholders. The system design automates gate access procedures, law enforcement personnel information access and status updates and visitor center passes. There are currently three DBIDS code bases deployed in different regions of the world due to unique requirements of the major commands. Another code base is under development to converge the application into one enterprise-wide identity management and force protection solution. Several types of workstations are employed in DBIDS, including:

Registration Station: Location where personnel data is collected, saved into the DBIDS database and DBIDS IDs can be issued. The current DBIDS Registration Station is a desktop workstation with peripherals including a 19" LCD flat-panel monitor, PVC printer (for credential printing), laser printer (credential approval and reporting), digital camera (desk-mounted tripod), fingerprint reader, 1D/2D pistol scanner/decoder (for barcodes 39 and PDF 417), and two smartcard readers. The Registration Station may include CrossMatch 1000 for capturing Ten-Print, Recognition System ID3D Handkey for capturing Hand Geometry, Securimetrics Pier 2.3 for capturing Iris image.

DMDC Computing Environments

Visitors Center: Location for sponsors to escort authorized persons and vehicles onto the installation.

Gate Workstations: Location where personnel and vehicles are verified, featuring remote, wireless hand scanning devices to assist security personnel in determining the identity and access privileges. The Gate and Visitor Center (VC) access point system includes a laptop or desktop workstation with a 19" LCD flat-panel monitor, uninterruptible power supply (UPS), laser printer, fingerprint reader, 1D/2D pistol scanner/decoder, smartcard reader, PDA handheld 1D scanners with a fingerprint reading attachment, battery-charging terminal, and spare batteries. Wireless communications between the guard shacks and the PDA handheld 1D scanners is provided by an 802.11b/g link utilizing a combination of 802.11b/g secured access points and high performance omni-directional and/or directional antennas (with lightning arrestors).

Law Enforcement Operations Workstation (LEO): Terminals that allow the Security Forces to search for the status and information of anyone or anything in the master database, to include escorted persons and vehicles. The Law Enforcement Office (LEO) station includes a workstation, 19" LCD flat-panel monitor, laser printer, fingerprint reader, 1D/2D pistol scanner/decoder, and a smartcard reader.

Servers: The servers are dual- or quad-processor based, with 2GB to 32GB memory complements (depending on usage), with multiple hard drives deployed in redundant arrays, and redundant power supplies. They can be deployed with individual 17" or 19" LCD flat-panel monitors, or can be connected to an existing KVM system provided by the host facility. Software on DBIDS workstations and servers includes Windows XP Professional and Windows 2003/2008 operating systems, a DoD-approved AntiVirus or HostBased Security System protection software, Aware's WSQ v2.34 compression software, DBIDS application (written using Microsoft Visual Studio), the Oracle client/server database products Oracle Data Sever/Enterprise/Standard Edition 10g/11g, Identix Fingerprint 1-to-1 Engine, and additional biometric SDKs and runtime applications as needed, such as the Aware NISTPack and Crystal Reports. The Gate and Visitor Center stations add the AirFortress encryption suite (Layer 2 security applications) or AirBEAM encryption suite (non-Layer 2 applications) for data transaction security between the PDA

DMDC Computing Environments

handheld scanner and the Gate/Visitor Center's host workstation. Guardian Edge disk encryption products are used to secure data at rest on the Gate and Visitor Center stations. CrossMatch Live Scan Management System 5.0, RSI Hand Geometry run time may be included. SQL Server Compact will be used on future versions of the DBIDS workstations in lieu of the Oracle database product.

Development and Testing Environment

DBIDS development is supported at the DMDC West facility in Seaside, CA on the Windows XP and Windows Server 2003 platforms. Microsoft Team Foundation Server recently replaced Microsoft Visual Source Safe as the source code repository. The development and testing system and network architecture includes:

Fourteen rack servers, three of which host 24 virtual servers under VMWARE Server or VMWARE ESX. Symantec NetBackup is used for backup and recovery. Sixteen blade servers will be deployed to expand capabilities in this environment. Eighty-eight Windows XP laptop or desktop workstations, on average each hosting three virtual Windows XP machines under VMWARE Workstation. Seven CISCO 3560/3570 switches, one Linksys SPS2024 switch and one Fortress Technologies AirFortress ES520 Secure Wireless Bridge. DBIDS software development is supported in this environment with the following products:

- Structured Query Language (SQL)
- Microsoft C/C++
- Microsoft Visual Basic
- Microsoft Visual Basic.NET
- Mobile Device Development on Microsoft Windows CE 5.0, Mobile 5.0 and future releases
- Oracle 10g/11g databases, PL/SQL, Oracle Designer, Oracle Enterprise Manager
- Smartcard middleware software
- Crystal Reports

DMDC Computing Environments

- DoD Information Assurance software products and tools (HBSS, Retina, DISA Gold Disk, and DISA Security Technical Implementation Guides (STIGs))
- Extensible Markup Language (XML) (including but not limited to Sun Microsystems XML Pack, Sun's Multi-Schema Validator (MSV), Simple Object Access Protocol (SOAP), and others), Extensible Schema Documents (XSD), and Document Type Definition (DTD)
- Secure Socket Layer
- SCRUM Methodology, Rational Unified Process Methodology, and Unified Modeling Language (UML)
- Compuware Optimal Trace for Requirement Documentation
- Biometric product and software integration (Fingerprint (single print and ten print), Hand Geometry, Iris, Photo)

Deployment Environment

Three DBIDS code bases are deployed throughout CONUS, Korea, Japan, Europe, and Southwest Asia. In CONUS, DBIDS is deployed to 27 military installations, each connecting to a Regional Data Center hosted at the DMDC West facility. The 27 installations have collectively deployed 82 Registration Stations, 36 LEO stations, 90 Gates, 37 Visitor Centers, and 20 Mobile Kits. The Regional Data Center system and network architecture includes:

- Ten blade servers, with a chassis with two integrated fibre channel switches
- One Cisco ASA5510 VPN Concentrator/Firewall
- A tape backup library
- A storage area network with integrate fibre channel switch
- Two Cisco 3650 switches

Currently, plans are to install DBIDS at 13 new sites in FY10, possibly 32 new sites in FY11, and possibly 4 new sites in FY12.

DMDC Computing Environments

Non-Combatant Evacuation Operations Tracking System (NTS) / Emergency Tracking and Accountability Tracking System (ETAS)

When a personnel evacuation is ordered due to military operations, political situations, natural disasters, or other potentially dangerous situations, NTS/ETAS assists with personnel tracking by providing visibility of evacuees, allowing support personnel to focus assets where needed to support the evacuation tracks the location of people and pets during the evacuation. Information required to identify each evacuee is collected during registration. Each evacuee is assigned a unique identifier that is used to track their location until they reach safe haven.

The ETAS establishes a local wireless LAN at each site that enables free-flow of information between all of the laptops on the network. Each registration station captures an Evacuee's information from their credential or via manual entry as necessary, and the evacuee is issued a bar coded bracelet. The local system stores all the information on an Oracle® relational database then periodically sends all the data to the main server, which maintains the data and pushes the information to a website. Evacuees are manifested via the bar coded bracelets at each site during the evacuation process. Movement information is forwarded to the gaining location by the server. Additionally, each evacuee may be located by performing queries via the server or the website by name or Evacuee ID number. Evacuees may include military family members, US Government employees and their families, other US citizens, and selected third country nationals (TCNs).

NTS/ETAS has two workstation types:

Registration System: Provides the capability to register an Evacuee into the NTS/ETAS and assigns a unique identifier (bar coded bracelet) for the purpose of tracking movement. Consists of a hardened case, laptop, credential scanners, and 3,000 bracelets. A passport reader is included with NTS, which is replaced by a Driver's License Scanner in ETAS.

Conveyance System: Provides the capability to manifest and track Evacuees using the barcode technology. Delivers query and report capability for the local commander and transfers data to a command center server. Also provides Satellite

DMDC Computing Environments

Communication, the access point for the wireless LAN, and a printer for manifests and reports. Includes one supply case.

Currently, there are 500 NTS kits deployed with military units throughout the world.

Environments.

DMDC provides development, quality assurance test, user acceptance test, and production environments for applications developed against the DEERS, ADR/ADW databases. The development, QA, and user acceptance test environments utilize a small representative subset of production like data. In certain cases applications are required to perform volume tests in a separate stress test environment which has a database equivalent in size and content to production. There are two development environments and two QA test environments to facilitate fixes to production while allowing development of the next set of releases. Applications are required to comply with a regular release schedule, unless it is an emergency. Production release to DEERS is monthly. User acceptance test release is weekly and must be approved by customer stakeholders. 85-90% of deployments to development and QA are automated and occur in minutes. The remainder generally occur within 24 hours